REMARKS

Reconsideration of the above-indicated patent application, as amended, is respectfully requested. The present amendment is responsive to the Office Action mailed April 5, 2004. Claims 1-24 have been rejected. Accordingly, amended claims and supporting remarks are hereby presented that particularly point out and distinctly claim the subject matter that applicant regards as the invention. No new matter has been added.

OBJECTION TO THE SPECIFICATION

The disclosure had been objected to for the blank spaces on page 13, lines 21 and 22 as originally filed. Accordingly, a substitute paragraph is included herewith identifying the application number and date of the related application.

THE REJECTIONS UNDER 35 U.S.C § 112

Claims 1-4, 9-12 and 17-20 had been rejected under Section 112, second paragraph, as being indefinite. The Examiner points out several instances in the claims where limitations had lacked sufficient antecedent basis. These instances are corrected herewith in the present amendment. It is therefore believed that this grounds of rejection is overcome, and reconsideration and withdrawal of this rejection is respectfully requested.

THE DISCLOSED EMBODIMENTS

As described in detail in the present specification, the present embodiments are directed to a method and apparatus for encryption and decryption of data. The embodiments include loading into a memory one or more encryption or decryption keys respectively associated with a first data frame, respectively including unencrypted or encrypted data. The key is comprised of a plurality of key values. The key is read out for a second data frame, simultaneously with the step of loading of key values into the memory. The step of reading out the key also respectively initiates an encryption or decryption operation using the key values loaded into memory to respectively encrypt or decrypt said second data frame. In this way, the encryption or decryption of a first data frame can be initiated while the encryption or decryption of a second data frame is being completed. This results in an efficient operation that greatly reduces processing time, since essentially two data frames are being processed simultaneously.

The benefits of these embodiments are preferably realized by the system including a dual port memory for storing in consecutive order a plurality of keys respectively associated with a plurality of data frames, as is the subject of certain groups of claims. The dual port memory is preferably included with a key RAM to house the key storage. This system includes a controller for initializing a table for encryption with at least one of the plurality of key values associated with a first data frame of the plurality of data frames. The controller commences initialization of the table prior to loading of all of the plurality of key values associated with the first data frame, and simultaneous with loading of key values. The controller also executes an algorithm to respectively encrypt or decrypt the first data frame using the initialized table. The controller respectively encrypts or decrypts the first data frame simultaneous with storing of key values associated with subsequent data frames of the plurality of data frames.

In this way, the dual ported memory allows a key to be loaded into a write port while simultaneously reading a key through a read port to initialize the table with the keys. As a result, the key for a second frame can be loaded into memory while simultaneously reading out the key for a first frame, without conflict. In this way, overlapping reading and writing is possible, which thereby reduces the key load/delay overhead of the second frame, since it is not necessary to wait for the processing of the first frame to be completed before starting to load the key for the second frame into memory. Key lookup is also improved since it may be possible to predict a forthcoming reception and have a particular key preloaded as indicated above. This removes the steps of looking up the proper key when the next frame arrives, thereby further accelerating processing and consequently improving efficiency. This is very different from the prior art relied on by the Examiner.

THE REJECTIONS UNDER 35 U.S.C § 103

Claims 1-24 had been rejected under Section 103 as being unpatentable over Newton in "Encyclopedia of Cryptology." This rejection is respectfully traversed, particularly as applied to the amended claims.

The Examiner states that the claims are rejected under Section 103(a) as being "anticipated" by Newton. It is respectfully submitted that this is a misstatement of the grounds of rejection, since a holding of anticipation can only be made under Section 102, not Section 103. It is respectfully requested that the Examiner withdraw and clarify this grounds of rejection and cite the appropriate sections of the patent law.

The Examiner states that Newton discloses loading into memory a plurality of keys simultaneously to decrypt a previous data frame. The basis for this statement is that Newton discloses using a previously decrypted letter as a key to decrypting the next letter, so that the key is "loaded" while decrypting the previous "data frame" or letter. The Examiner admits that Newton fails to disclose using such a method on a computer system, but takes official notice that encryption algorithms are commonly used on computer systems.

This grounds of rejection is not well taken. It is noted that the citation relied upon, the "Priming Key" section from page 223 of the reference, is simply a two-paragraph section describing a manual cryptographic technique developed by Blaise de Vigenere in the late 1500s. This citation can only be construed as being of the most general nature. This thin disclosure can hardly be relied upon to satisfy the requirements of the present claims. And it is a very casual dismissal of the claim limitations to simply assert that the claims are satisfied by implementing a medieval technique in a modern computer system.

Specifically, the claims recite steps and structure directed to "loading into a memory" respective encryption and decryption keys. The claims further require "reading out a key ... simultaneously with the step of loading." These are specific steps that cannot generally be encompassed by the simple notion of computer-implementing a manual method. Such goes beyond the teachings of the reference and could not be arrived at without a hindsight reading of the present disclosure. Still further, the term "data frame" as used in the claims is a well-known term of art in the field of communications, akin to the term "data packet." Thus, it is improper to equate a "data frame" as presently recited with a "letter" in the manual method of de Vigenere, particularly without a proper citation of a reference.

The arrangement disclosed by Newton is otherwise very different from the current invention since it does not rely on “using the previously decrypted letter as a key to decrypt the next letter”. Such a dependency does not exist in this application. This would imply the key update for the next frame always depends on the result of the current frame. However, the key being used to decrypt and the key being loaded (written) may be used for different data frames being sent to/from different clients. Hence there is no dependency. For example, a key at RAM address 10 may be used for **encrypting** traffic to client 10 and key in position 20 used to decrypt traffic from client 20.

Encryption key management is often performed by a processor that runs (commonly called Key Server in the art) application software which writes keys as the client information database for encrypt/decrypt is updated. This is typically done on as an upper networking layer application, whereas encryption/decryption occurs at the lower MAC layer. It should be understood that key updates can happen quite frequently in an embedded environment as wireless clients roam to different access points. It should also be appreciated that to provide acceptable quality of service in fast roaming application handoff such as Wireless Voice Over IP (VOIP), there is the potential for a time critical need. Furthermore added security is popular lately requiring larger key sizes (approaching up to 256 bits with AES for example), hence efficient key loading is important.

This software key loading happens in the background simultaneously with yet another process (often done by hardware) handles the reading of keys for encryption/decryption for the current wireless frame being actively transported across the wireless LAN. These two different hardware and software process are unaware of the state of each other and hence both can operate without having to arbitrate or contend for access to the common key memory. This is a key advantage of the current invention brought about by the dual ported nature of the key storage. Referring to the above example, key number 10 could be used actively by the hardware to decrypt a packet, meanwhile software can freely write key number 20 for a new client that is authenticated and associated to the wireless network. This software update does not impact the time critical hardware nature of the decryption operation. Nor does hardware impact the efficient key loading of the de-coupled software process. Both processes can peacefully co-exist on the same common dual ported key memory.

Still further, other computer specific limitations are recited in the present claims, such as a "table for encryption or decryption," a "dual port memory," and a "controller for executing an algorithm." It is plain that such limitations cannot be found within the four corners of Newton, nor can anything be inferred from this reference that would suggest the desirability of the presently claimed limitations. Indeed, it is again clear that the present claims could not be arrived at from Newton unless guided by the teachings of the present disclosure. Nonetheless, in the interest of advancing prosecution, claims 1-4, 9-12, 17 and 19 have been amended to more particular point out and distinctly claim the subject matter applicant regards as the invention.

In view of the foregoing it is respectfully submitted that the present claims, as currently amended, distinguish over the prior art. A notice to that effect is earnestly solicited. If the Examiner believes there are any further matters, which need to be discussed in order to expedite the prosecution of the present application, the Examiner is invited to contact the undersigned.

Respectfully submitted,

TUCKER ELLIS & WEST LLP

Jay P. Ryan
Agent for Applicant
(Registration No. 37,064)
1150 Huntington Building
925 Euclid Avenue
Cleveland, Ohio 44115-1475
Customer No. 23380
216-696-4396 (phone)
216-592-5009 (fax)